Ekwan E. Rhow (CA SBN 174604)
erhow@birdmarella.com
Marc E. Masters (CA SBN 208375)
mmasters@birdmarella.com
Christopher J. Lee (CA SBN 322140)
clee@birdmarella.com
BIRD, MARELLA, RHOW, LINCENBERG, DROOKS & NESSIM, LLP
1875 Century Park East, 23rd Floor
Los Angeles, California 90067-2561
Telephone: (310) 201-2100
Facsimile: (310) 201-2110

Jonathan M. Rotter (CA SBN 234137)
Kara M. Wolke (CA SBN 241521)
Gregory B. Linkh (pro hac vice)
GLANCY PRONGAY & MURRAY, LLP
1925 Century Park East, Suite 2100
Los Angeles, California 90067-2561
Telephone: (310) 201-9150
jrotter@glancylaw.com
kwolke@glancylaw.com
glinkh@glancylaw.com

Attorneys for Plaintiffs

Kalpana Srinivasan (CA SBN 237460)
Steven Sklaver (CA SBN 237612)
Michael Gervais (CA SBN 330731)
SUSMAN GODFREY L.L.P.
1900 Avenue of the Stars
14th Floor
Los Angeles, CA 90067
Telephone: (310) 789-3100
ksrinivasan@susmangodfrey.com
ssklaver@susmangodfrey.com
mgervais@susmangodfrey.com

Y. Gloria Park (*pro hac vice*)
SUSMAN GODFREY L.L.P.
One Manhattan West
50th Floor
New York, NY 10001
Telephone: (212) 336-8330
gpark@susmangodfrey.com

John W. McCauley (*pro hac vice*)
SUSMAN GODFREY L.L.P.
1000 Louisiana Street, Suite 5100
Houston, TX 77002
Telephone: (713) 651-9366
Facsimile: (713) 654-6666
jmccauley@susmangodfrey.com

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

BERNADINE GRIFFITH; et al., individually and on behalf of all others similarly situated,

Plaintiffs,

vs.

TIKTOK, INC., a corporation; BYTEDANCE, INC., a corporation

Defendants.

Case No. 5:23-cv-00964-SB-E

PLAINTIFFS' REPLY MEMORANDUM IN FURTHER SUPPORT OF THEIR MOTION FOR CLASS CERTIFICATION

REDACTED VERSION OF DOCUMENT PROPOSED TO BE FILED UNDER SEAL

JUDGE: Hon. Stanley Blumenfeld, Jr.
DATE: August 16, 2024
COURTROOM:
350 West 1st Street
Los Angeles, CA 90012
Courtroom 6C

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

TABLE OF ABBREVIATIONS

EAPI	Events API
Ex. 1-35	Exhibits to the Park Declaration in Support of Plaintiffs' Motion for Class Certification (Dkt. 177-8)
Ex. 36-46	Exhibits to the Park Declaration in Support of Reply Memorandum in Further Support of Plaintiffs' Motion for Class Certification (filed concurrently with this Reply Memorandum)
Li ¶ __	Declaration of Lizzie Li in Support of Opposition to Motion for Class Certification (Dkt. 195-1)
Mangum ¶ __	Declaration of Russell W. Mangum III, Ph.D., in Support of Plaintiffs' Motion for Class Certification (Dkt. 179-3)
Mangum Reply ¶ __	Declaration of Russell W. Mangum III, Ph.D., in Support of Plaintiffs' Reply in Support of Motion for Class Certification (filed concurrently with this Reply Memorandum)
Opening __	Plaintiffs' Memorandum of Points and Authorities in Support of Their Motion for Class Certification (Dkt. 179-1)
Opp. __	Defendants' Opposition to Plaintiffs' Motion for Class Certification (Dkt. 195)
Schnell ¶ __	Declaration of Ron Schnell (Dkt. 195-16)
Shafiq ¶ __	Declaration of Zubair Shafiq, Ph.D., in Support of Plaintiffs' Motion for Class Certification (Dkt. 179-2)
Shafiq Reply ¶ __	Expert Reply Declaration of Zubair Shafiq, Ph.D., in Support of Plaintiffs' Motion for Class Certification (filed concurrently with this Reply Memorandum)

Defendants uniformly and automatically collect baseline data from everyone who visits a non-TikTok website that uses the Pixel or EAPI. Defendants downplay this as "the mere collection of browsing data," Opp. 1, and pretend that the only actionable conduct is the collection of [redacted]. This is not true. In any event, that is a merits question.

The relevant inquiry at this stage is not whether Defendants' conduct is legal, but whether that question is capable of class-wide resolution. It is. The Court should certify the proposed classes.

A. Defendants' Concessions.

Defendants concede that California law applies nationwide, the classes are sufficiently numerous, and Plaintiffs' counsel are adequate. *Rozier v. Dep't of Homeland Sec. Fed. Protective Serv.*, 2022 WL 2199938, at *3 (C.D. Cal. Mar. 7, 2022).

B. Plaintiffs' Class Definitions Are Appropriate.

The classes are not "overbroad." Opp. 7. Plaintiffs seek to certify classes of non-TikTok users whose data Defendants intercepted from websites that use the Pixel (Class 1). Opening 2-3 (describing additional classes). Defendants and their technical expert, Mr. Schnell, do not dispute that even without any configuration from websites with the Pixel installed, TikTok sets PageView as a default event, then uniformly and automatically collects Timestamp, IP Address, User Agent, Cookies, URLs, Event Information, and Content Information ("Default Data"). Opening 8; Shafiq Reply ¶¶60-62; Ex. 38 (30:12-14, 124:18-22).[1] Defendants do not dispute Plaintiffs' expert Dr. Shafiq's finding that 2,000 random websites that use the Pixel collected all seven

[1] Unable to dispute that the Pixel automatically collects Default Data, Defendants and Mr. Schnell argue that such collection is "industry-standard" and just "the way the Internet works." Opp. 1; Schnell ¶¶33, 44. Wrong. Unlike other pixels on the market that limit collection, TikTok purposefully chooses to collect Default Data. Shafiq Reply ¶¶24-36.

categories of Default Data nearly 100% of the time. Shafiq ¶¶76-80, Shafiq Reply ¶¶60-62.

Defendants assert that [redacted]. Opp. 9, 11.[2] But Defendants automatically and uniformly also collect IP Address, User Agent, and Cookies, which are identifiers in their own right. Shafiq ¶¶47-66; Shafiq Reply ¶¶75-79. Defendants also collect [redacted]. As the FTC warns, despite some companies' claims otherwise, hashed data is trivially reversible and identifying. Shafiq Reply ¶¶79, 88.

Second, Defendants argue that [redacted]. Opp. 9. This misses the mark. Extrapolating from Defendants' sample—consisting of data collected in under one hour—implies that they collect [redacted]. Shafiq Reply ¶¶82-84. And full-string URLs, which Defendants concededly collect (*e.g.*, Schnell ¶¶33, 72), are sensitive even when they do not contain [redacted]. They often transmit other sensitive data via the domain itself and in the context of broader browsing history and identifying information collected by TikTok. Shafiq Reply ¶¶87-91.

Defendants' cases (Opp. 8) support certification. In *United States v. Forrester*, the collection of IP addresses was constitutional only because they did not reveal "the contents of the messages" or "the websites the person viewed." 512 F.3d 500, 510 (9th Cir. 2008). *In re Zynga Privacy Litigation,* 750 F.3d 1098, 1107-09 (9th Cir.

[2] Defendants' claim that [redacted] (Opp. 10; *see also id.* at 14) is demonstrably false and reeks of gamesmanship. First, the SAC identifies Etsy, and Dr. Shafiq found [redacted]. *See* Shafiq ¶63(vi). Second, Defendants conveniently omit that the sample they produced was from under an hour and does not remotely encompass all the class-member data collected during the class period. Indeed, Defendants purposely deleted most of that data. Plaintiffs will separately file a motion seeking relief from Defendants' simultaneous deletion of class-member data and weaponization of the resulting absence of data.

2014), found the collection of referer headers lawful only because they did not contain the kind of information contained in full URLs. The Ninth Circuit distinguished *Forrester* and *Zynga* in *In re Facebook Internet Tracking Litigation* because Facebook collected "full-string detailed URL," the "full referral URL," and "correlate[d] that URL" with identifying information. 956 F.3d 589, 604-05 (9th Cir. 2020). TikTok uniformly collects the same type of information here, making this case like *Facebook Tracking* and unlike *Forrester* and *Zynga*. Defendants purposefully design the Pixel to collect information not only from the Referer header (like in *Zynga*) but also from the HTTP payload (which allows it to collect full-string referer URLs even when websites try to limit that transmission)—not to mention event listeners that scrape metadata and follow around every mouse movement on a webpage to infer button clicks. Shafiq Reply ¶¶30-31 & Figs. 1&2; Shafiq ¶¶64-66. The full-string URLs and button clicks that TikTok collects are "content." *See In re Meta Pixel Healthcare Litig.*, 647 F.Supp.3d 778, 795 (N.D. Cal. 2022); *Hammerling v. Google LLC*, 615 F.Supp.3d 1069, 1089 (N.D. Cal. 2022) (that Google allegedly collected usage data across non-Google apps sufficient to allege reasonable expectation of privacy); *Griffith v. TikTok, Inc.*, 697 F.Supp.3d 963, 975-76 (C.D. Cal. Oct. 6, 2023) (rebuking Defendants' reliance on outdated *Low v. LinkedIn Corp.*, 900 F.Supp.2d 1010 (N.D. Cal. 2012)).

Even accepting Defendants' myopic framing of the facts, the "factual issues" are not "individualized." Opp. 9. First, for the privacy and seclusion claims, even if the "data must be identifying and sensitive,"[3] Opp. 8, that inquiry can be conducted in a programmatic, class-wide basis. Shafiq Reply ¶¶82-84, 93-94. Second, for the CIPA and ECPA claims, even if the full-string URL "must contain particular information like search terms" to constitute "contents," Opp. 8, Dr. Shafiq has already written a program that can programmatically identify search terms in URLs.

[3] But *Facebook Tracking* actually ***rejected*** Facebook's argument that "Plaintiffs need to identify specific, sensitive information that Facebook collected." 956 F.3d at 603.

Shafiq ¶63(vi) & App'x B. Third, whether class members "have some recognized basis to exclude others from that information" is a class-wide inquiry of whether they have a reasonable expectation that Defendants would not collect their data from non-TikTok websites. *See Griffith*, 697 F.Supp.3d at 971.

C. Plaintiffs Satisfy Rule 23(a).

1. Commonality

The existence of "a single common question" of fact or law satisfies commonality under Rule 23(a). *See Franklin v. Midwest Recovery Sys., LLC*, 2021 WL 1035121, at *2 (C.D. Cal. Feb. 5, 2021). The questions that Defendants themselves identify—"(1) whether information was disclosed to TTI and (2) the nature of the information," Opp. 11—are common questions. On Defendants' first question, Dr. Shafiq's testing on 2,000 randomly selected websites shows that six of seven categories of Default Data "w[ere] disclosed to TTI" 100% of the time and Content Information nearly 98% of the time. Shafiq ¶¶77-80. There is no substantial variability across websites, [redacted]. Shafiq ¶¶76-86; Shafiq Reply ¶¶62-74.

On Defendants' second question, all data points collected include, as a baseline, identifying fields (IP Address, User Agent, Cookies, email and phone either hashed or unhashed) and sensitive content (URL, Event Information, Content Information). Shafiq ¶¶47-66. That the data collected is identifying and sensitive is particularly true where one looks at each collected data point in context of the overall browsing history collected from countless websites. Shafiq Reply ¶¶89-91. Defendants cite zero authority for their claim that the Court must look at each data point in isolation to see whether it contains both identifying and sensitive information.

Defendants attempt to blame the websites who use the Pixel for Defendants' unlawful conduct, Opp. p.11, but such finger-pointing does not preclude certification. *First*, Defendants start with the truism that [redacted]

This doesn't get Defendants far because [redacted] Shafiq ¶63. *Second*, Defendants say [redacted] but regardless of how the website configures its URL, Defendants could choose not to collect sensitive content from that URL. Ex. 39 (90:6-17); Shafiq Reply ¶¶30-32. They choose to collect it.

Third, Defendants fixate on the fact that "advertisers decide whether to install [Pixel] on every page of its website or on certain pages," noting that the Pixel (***currently***) is installed on riteaid.com but not on riteaid.com/pharmacy. Opp. 11, 13; Shafiq Reply ¶108; Ex. 38 (143:20-24) ([redacted]). Even in the rare circumstance where the Pixel is not installed on every webpage, it is typically installed on the homepage. Using the RiteAid example, this means that TikTok collects class-member data when they visit "riteaid.com" even before they navigate to the pharmacy subpage. Dr. Shafiq found the Pixel installed on 100% of the homepages of the 2,000 randomly sampled websites he tested. Shafiq Reply ¶110. [4]

As to "individualized issues" via "class member interactions," Opp. 11-12, Defendants tout "many privacy protection options, such as cookie blockers or other privacy controls" but fail to acknowledge sources cited by their own expert, which show that the most popular adblockers on the market do not block the TikTok Pixel's transmissions. Shafiq Reply ¶112 & nn.188-191. Even if they did, [redacted]. Shafiq ¶39.

2. Typicality and Adequacy

"Typicality refers to the nature of the claim or defense of the class representative, and not the specific facts from which it arose or the relief sought."

[4] If the Court finds Defendants' argument persuasive, then the class definition can be modified to refer to "webpage" instead of "website" pursuant to the Court's inherent authority to "redefine the class to bring it within the scope of Rule 23." 7A Wright & Miller, Federal Practice and Procedure § 1759 (4th ed. 2023).

Abels v. JBC Legal Grp., P.C., 227 F.R.D. 541, 545 (N.D. Cal. 2005) (citation omitted).

Defendants' scattershot arguments attacking typicality and adequacy all fail. First, Defendants are wrong that Plaintiffs "cannot represent visitors to websites they themselves never visited." Opp. 13. All the websites at issue employ common software, which collects a common set of Default Data. The collection does not vary from one website to the next. Shafiq ¶¶76-80. This satisfies typicality. *Chavez v. Blue Sky Nat. Beverage Co*., 268 F.R.D. 365, 377-78 (N.D. Cal. 2010). Alternatively, Plaintiffs may represent the proposed website-specific classes.

Second, there are no "divergent interests" among class members (Opp. 13): Whether they ordered McDonalds from Doordash or made a medical appointment, they have a shared common interest in not having their data intercepted or used by Defendants.

Third, Plaintiffs have standing, and Defendants are factually incorrect that Plaintiffs "have not shown a disclosure" of their data to Defendants. Opp. 14. Plaintiffs submitted declarations that they visited websites using the Pixel and EAPI during the class period. Dkts. 177-2, 177-3, 177-4. That establishes standing. *See Van v. LLR, Inc.*, 61 F.4th 1053, 1064 (9th Cir. 2023) (even "trifling" injury suffices).

Fourth, for the reasons discussed below, *infra* Sec. E, Defendants have not shown consent.

D. Plaintiffs Satisfy Rule 23(b)(3).

Defendants' attacks on predominance are likewise unavailing. To satisfy predominance, "a plaintiff need not rebut every individualized issue that could possibly be raised. To demand such proof would be akin to demanding proof 'that plaintiffs would win at trial.'" *Van*, 61 F.4th at 1066 (citation omitted).

1. Privacy and Seclusion

Common questions predominate for both elements of Plaintiffs' privacy and seclusion claims, and Defendants' argument to the contrary ignores black-letter law.

"[W]hether someone has a reasonable expectation of privacy is an objective, and therefore common, inquiry." *In re Google RTB Consumer Priv. Litig.*, 2024 WL 2242690, at *5 (N.D. Cal. Apr. 4, 2024); *Rodriguez*, 2024 WL 38302, at *4 (reasonable expectation of privacy is "objective"; judged by "reasonable person" standard); *Brown v. Google LLC*, 685 F.Supp.3d 909, 941 (N.D. Cal. Aug 7, 2023) (same). By definition, an objective standard obviates the need to examine plaintiffs' subjective expectations. *E.g. Opperman v. Path*, 2016 WL 3844326, at *11 (N.D. Cal. Jul. 15, 2016).

To determine whether there was a reasonable expectation of privacy, the factfinder should consider "the identity of the intruder," "the extent to which other persons had access to the subject place," and "the means by which the intrusion occurred." *Hernandez v. Hillsides, Inc.*, 47 Cal.4th 272, 286-87 (2009). Those are common issues, focusing on "the intruder's motives and objectives" and "the degree and setting of the intrusion." *Id.* These factors do not involve analysis of the plaintiffs' attributes. *Id.* at 288-300.[5]

As to the offensiveness of intrusion, internally, [redacted], *see* Opening 11-12, which Defendants try to write off as [redacted] Opp. 17. Quite the contrary: Dr. Shafiq shows that Defendants could avoid the collection of Default Data, as other tracking pixels do. Shafiq Reply ¶¶24-36. They choose not to.

Defendants' cases do not prevent certification. *McDonald v. Kiloo Aps*, 385 F.Supp.3d 1022, 1035 (N.D. Cal. 2019) (cited in Opp. 17), actually ***sustained*** privacy claims, noting that "[c]urrent privacy expectations are developing" about "whether a commercial entity that secretly harvests [data] commits a highly offensive or egregious act." By contrast, there was no secret data harvesting in *Hart v. TWC Prod.*

[5] Because the privacy claims involve an "objective" standard, Defendants' arguments that "[d]ifferent websites with different content, practices, and user interactions raise different privacy concerns," Opp. 13, don't matter. Dr. Stivers' analysis is irrelevant at this stage. Plaintiffs will address Dr. Stivers' flawed findings in due course.

& Tech. LLC, 2023 WL 3568078, at *11 (N.D. Cal. Mar. 30, 2023); TWC's policy "explicitly disclosed the practices at issue," as did a "panoply" of other sources. *In re Toll Rds. Litig.*, 2018 WL 4945531, at *7 (C.D. Cal. Oct. 3, 2018), where the court certified a Rule 23(b)(3) class, did not involve online data harvesting at all. *Cf. Rodriguez*, 2024 WL 38302, at *5 (distinguishing *Hart* and granting certification).

2. CIPA and ECPA

Defendants preview their merits arguments about the "contents" and "in transit" requirements (Opp. 18-19) and, in the process, unwittingly concede the class-wide nature of the inquiries about the data collection.

"Contents," under ECPA, is "any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510; *Brodsky v. Apple Inc.*, 445 F.Supp.3d 110, 127 (N.D. Cal. 2020) (same under CIPA). Whether URLs constitute "contents" under these statutes is a common question. *See* Opening 13-15. Whether Event Information and Content Information—which reveal what someone is doing, viewing, and clicking, Shafiq ¶¶56, 64-65—constitute "contents" is also a class-wide inquiry.

While Plaintiffs dispute Defendants' [redacted] *accord* Shafiq Reply ¶¶95-102, the operation of the Pixel and EAPI either does or does not meet the "contemporaneous" and "in transit" requirements. Defendants argue that this inquiry "require[s] a close look at each configuration," Opp. 19, yet they [redacted]. Shafiq ¶32; Shafiq Reply ¶55-57. There is no evidence in the record that websites deviate from this [redacted].

3. Larceny and Conversion

Defendants' arguments about these claims relitigate issues already decided by the Court. *Griffith*, 697 F.Supp.3d at 976 ("Defendants have not shown as a matter

of law that Plaintiff's allegation that she had a property right in the data Defendants collected is implausible"). Regardless, that is capable of class-wide resolution.

4. Damages

Disgorgement: Defendants' arguments about Plaintiffs' disgorgement theories go to the applicability or amount of disgorgement, which are common issues. The "partitioning of damages among class members may lead to individual calculations," but "those calculations would not impact a defendant's liability for the total amount of damages," and they "do not defeat certification." *Ruiz Torres v. Mercer Canyons*, 835 F.3d 1125, 1140-41 (9th Cir. 2016). Defendants also lack standing to criticize the method of apportioning disgorgement. *Brown v. Google LLC*, 2022 WL 17961497, at *7 (N.D. Cal. Dec. 12, 2022).

In any event, Defendants' argument that Plaintiffs must demonstrate the "net profit . . . attributable to the underlying wrong," Opp. 20, contradicts the law. Once Plaintiffs "present evidence of the total or gross amount of the benefit," the burden shifts to Defendants to show "costs, expenses, and other deductions to show the accrual or net benefit the defendant received." *Brown*, 2022 WL 17961497, at *6. Defendants have not met their burden. Nor can they, where testimony from Defendants' own experts and employees demonstrates that the Pixel cannot operate at all without collecting class-member data. Mangum Reply ¶¶11-18.

Actual Damages: Undercutting Defendants' baseless assertion that Plaintiffs provided no method to determine actual damages (Opp. 21) is the fact that Plaintiffs' model is similar to the one endorsed in *Rodriguez*. 2024 WL 38302, at *11-12. *See* Opening 19; Mangum ¶¶85-123. Defendants' argument that "[a]ny valuation requires comparing how much and what data was collected from each class member," Opp. 21, ignores that the market measures used by Dr. Mangum do not pay consumers based on how much or what data is collected. Mangum Reply ¶¶21-29. Even if calculating actual damages requires "comparing how much and what data was collected from each class member" (it doesn't), that ***still*** would not defeat

certification. *See In re Lidoderm Antitrust Litig.*, 2017 WL 679367, at *25 (N.D. Cal. Feb. 21, 2017).

Statutory Damages: While TikTok mentions the "discretionary" nature of statutory damages, Opp. 21, their availability is a common question. Disparity in damages claimed by representatives and other class members doesn't preclude certification. *Santoro v. Aargon Agency, Inc.*, 252 F.R.D. 675, 681 (D. Nev. 2008), *as corrected* (Oct. 21, 2008).

E. Defendants Fail to Establish Individual Issues of Consent.

"While Plaintiffs bear the burden of proving predominance under 23(b)(3), [TikTok] bears the burden of proof for the affirmative defense of consent." *Rodriguez*, 2024 WL 38302, at *8; *see* Opening 17 (applicable legal standard). When assessing predominance, courts "do not consider the consent defenses … for which [a defendant] has presented no evidence." *True Health Chiropractic, Inc. v. McKesson Corp.*, 896 F.3d 923, 932 (9th Cir. 2018).

Defendants present no evidence of express consent. Class members have no reason to know that when they browse websites, Defendants take and use their data. This Court already found that the privacy policies of the websites identified in the complaint failed to establish even "awareness," let alone consent. *Griffith*, 697 F.Supp.3d at 972.

The same is true of all websites that use the Pixel and EAPI. In response to an interrogatory to identify all websites that "specifically disclosed the Website's usage of the TikTok Pixel and/or the TikTok Events API and the collection of data specifically by TikTok and/or ByteDance," Defendants refused to identify a single website. Ex. 36. Defendants' corporate representative [redacted]. Ex. 41 (264:4-13).

Defendants for the first time identity ***two*** websites, which they claim notify visitors of the Pixel. Opp. 6. But those disclosures fall short. Neither mentions EAPI or ByteDance. Every Man Jack says "we use the TikTok Pixel" but does not explain

that it collects data on non-TikTok users, and it refers readers to "TikTok's ***user*** privacy policy" for more information. *See* Opp. 6 n.2. Bump Box identifies TikTok cookies but does not explain what they do. *See id.* n.3. Neither "convincingly show[s] that the party knew about and consented to" Defendants' collection of Default Data from non-TikTok users. *In re Gmail*, 2014 WL 1102660, at *16 (N.D. Cal. Mar. 18, 2014).

Defendants likewise do not enforce any purported disclosure "requirement." *See* Ex. 42 (332:20-333:3); Ex. 41 (166:17-18, 164:16-165:8). Defendants' expert testified that [redacted] Ex. 38 (98:13-22). [redacted]. *Id.* (67:13-77:13; 82:2-83:19); Li ¶11. [redacted]. Ex. 43 at -7689-7691.

Implied consent also fails. Defendants claim that, by continuing to visit websites that use the Pixel or EAPI, plaintiffs impliedly consented to Defendants' receipt of their data. Opp. 19-20. *Rodriguez* forecloses this argument: "It is unreasonable for Google to expect, as it does, that users must also stop using the many apps on their phone . . . to show a lack of consent." 2024 WL 38302, at *5. The argument applies with even greater force here, where class members ***do not even know*** which websites use the Pixel or EAPI (and Defendants designated the list of websites as Attorneys' Eyes Only to preclude even Plaintiffs' access). For the few websites they did know used the Pixel or EAPI, Plaintiffs testified that they tried to be aware of, avoid, or limit using them. Ex. 44 (345:17); Ex. 45 (255:18-19); Ex. 46 (282:11-14). Crediting Defendants' implied-consent theory would require non-TikTok users to stop using the Internet altogether.

Defendants cannot rely on *Google RTB* or *Brown* because they have not shown any evidence of consent. *See Google RTB,* 2024 WL 2242690, at *12-14 (specific

disclosures to account holders, language in Google's privacy policy, surveys); *Brown*, 2022 WL 17961497, at *17-19 (specific language from privacy policy, other notices, survey, media and academic reports, and hyperlink on the Incognito screen clicked more than 14 million times).

F. Defendants' Arguments about Ascertainability and Superiority Are Misplaced.

Defendants argue that "class membership is individualized" because "[s]elf-reporting is unreliable." Opp. 15. But plaintiffs need not establish ascertainability. *Briseno v. ConAgra Foods, Inc.*, 844 F.3d 1121, 1133 (9th Cir. 2017). Defendants' cases questioning self-identification pre-date *Briseno*. Opp. 15-16.

Defendants complain that they cannot verify class members' identities against their own records, Opp. 16, but Defendants created that issue by purposely deleting class-member data. "[C]ourts generally do not bar class certification where the defendant's own destruction of records causes difficulty in identifying class members." *Raffin v. Medicredit, Inc.*, 2017 WL 131745, at *6 n.5 (C.D. Cal. Jan. 3, 2017).

Defendants also complain about determining "specific pages with the Pixel" or "the period it was used," Opp. 22, but Defendants possess this information. Class members need only confirm that they visited a website with the Pixel during the relevant time. Whether a class member visited a particular webpage with the Pixel is an issue not of identification but of damages. Even if some class members have no damages, the presence of even a greater than *de minimis* number of "uninjured" class members does not bar certification. *Olean Wholesale Grocery Coop., Inc. v. Bumble Bee Foods LLC*, 31 F.4th 651, 669 (9th Cir. 2022).

Finally, whether or not "a website may have multiple pixels with changing settings running simultaneously," Default Data is always taken, obviating individualized inquiry. Defendants' assertion that there would be individual determination of "whether the data disclosure included personal, sensitive, or

substantive information" misstates the law. *Supra* n.3. Nevertheless, Dr. Shafiq explains how the data can be linked to individuals. Shafiq Reply ¶¶75-79, 87-88.

G. The Court Should Certify an Injunctive Class.

Defendants' conclusory claim that injunctive relief affects class members differently is meritless. Opp. 22-23, Defendants collect and use Default Data from every class member. Plaintiffs seek to enjoin that common practice and Defendants' ongoing use of class-member data, including products or algorithms built with that data. *E.g. United States v. Kurbo, Inc.*, No. 3:22-cv-946, Dkt. 15 at II.D (N.D. Cal. Mar. 3, 2022).

Further, Defendants continue to collect class-member data, so there will be future injury to class members absent injunctive relief. Defendants have not satisfied their burden regarding the defense of consent, and such argument is particularly improper concerning injunctive relief where Defendants have identified in this litigation hundreds of thousands of websites that have used the Pixel. That information is not publicly available to class members (or even to Plaintiffs). Short of steering clear of the Internet altogether, Plaintiffs could not avoid Defendants' improper data collection without injunctive relief. *Rodriguez*, 2023 WL 38302, at *5.

Dated: July 26, 2024

By: /s/ *Ekwan E. Rhow*

Ekwan E. Rhow (CA SBN 174604)
Marc E. Masters (CA SBN 208375)
Christopher J. Lee (CA SBN 322140)
BIRD, MARELLA, RHOW, LINCENBERG, DROOKS & NESSIM, LLP
1875 Century Park East, 23rd Floor
Los Angeles, California 90067-2561
Telephone: (310) 201-2100
erhow@birdmarella.com
mmasters@birdmarella.com
clee@birdmarella.com

Jonathan M. Rotter (CA SBN 234137)
Kara M. Wolke (CA SBN 241521)
Gregory B. Linkh (*pro hac vice*)
GLANCY PRONGAY & MURRAY, LLP

1925 Century Park East, Suite 2100
Los Angeles, California 90067-2561
Telephone: (310) 201-9150
jrotter@glancylaw.com
kwolke@glancylaw.com
glinkh@glancylaw.com

Kalpana Srinivasan (CA SBN 237460)
Steven Sklaver (CA SBN 237612)
Michael Gervais (CA SBN 330731)
SUSMAN GODFREY L.L.P.
1900 Avenue of the Stars, Suite 1400
Los Angeles, CA 90067
Telephone: (310) 789-3100
Facsimile: (310) 789-3150
ksrinivasan@susmangodfrey.com
ssklaver@susmangodfrey.com
mgervais@susmangodfrey.com

Y. Gloria Park (pro hac vice)
SUSMAN GODFREY L.L.P.
One Manhattan West
50th Floor
Telephone: (212) 336-8330
Facsimile: (310) 336-8340
gpark@susmangodfrey.com

John W. McCauley (*pro hac vice*)
SUSMAN GODFREY L.L.P.
1000 Louisiana Street, Suite 5100
Houston, TX 77002
Telephone: (713) 651-9366
Facsimile: (713) 654-6666
jmccauley@susmangodfrey.com

Attorneys for Plaintiffs

CERTIFICATE OF COMPLIANCE

The undersigned counsel of record for Plaintiffs certifies that this brief contains 4,000 words, which complies with the word limit of Rule 6(c)(i) of Judge Stanley Blumenfeld, Jr.'s Standing Order for Civil Cases.

/s/ Gloria Park
Gloria Park

CERTIFICATE OF SERVICE

I, the undersigned say:

I am not a party to the above case, and am over eighteen years old. On July 26, 2024, I caused to be served true and correct copies of the foregoing document, by posting the document electronically to the ECF website of the United States District Court for the Central District of California, for receipt electronically by the parties listed on the Court's Service List.

I affirm under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on July 26, 2024, at New York, NY.

/s/ Gloria Park
Gloria Park